UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,952	09/20/2000	John S. Roman	END9-1999-0107	7354

21254 7590 06/07/2004

MCGINN & GIBB, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
ZIA, MOSSADEQ	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 06/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/666,952	**Applicant(s)** ROMAN ET AL.	
	Examiner Mossadeq Zia	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 4-9, 19, 22-27 are rejected under 35 U.S.C. 102(b) as anticipated by Patent No. 5,937,159, Meyers et al.

3. Regarding claims 1, 19, Meyers shows a method for controlling access to a computer system comprising:

classifying applications running on an untrusted computer system (non-TCB program, Meyers, col. 11, line 12-13) as running in one of a trusted application execution context (security attributes, Meyers, line 11, line 34-36) and an untrusted application execution context (name of service, Meyers, col. 12, line 51-52); and

preventing an application on said untrusted computer system from initiating a connection with a trusted computer system unless said untrusted computer system is running said application in said trusted application execution context (Meyers, col. 12, line 18-20).

4. Regarding claim 4, 22 Meyers show claim 1 above, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names (name of service, Meyers, col. 12, line 51-52).

5. Regarding claims 5, 23 Meyers discloses claim 4 above, and further showshow a human administrator of said untrusted system assigns said distinctive application execution context names (Meyers, col. 6, line 29-30).

6. Regarding claims 6, 24, Meyers shows claim 4 and 14 above, and further show said applications cannot change the names of respective execution contexts in which said applications are running (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

7. Regarding claims 7, 25, Meyers shows claim 4 and 14 above, and further show said applications cannot change the name of any execution context in said untrusted computer system (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

8. Regarding claims 8, 26, Meyers shows claim 1 and 10, above, wherein connections originating on said external system can terminate only at said untrusted system and only at said untrusted execution contexts therein (Session monitor, Meyers, col. 7, line 30-34).

9. Regarding claims 9, 27, Meyers shows claim 1 and 10 above, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system (System Boundary, Meyers, col. 4, line 66-67).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 2, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,937,159, Meyers et al. in view of "SIGMA: Security for Distributed Object Interoperability Between Trusted and Untrusted Systems", Sebes et al.

12. Regarding claim 2, Meyers shows claim 1 above, but fail to show said trusted computer system can initiate connections with any execution context on said untrusted computer system.

However, Sebes teaches another possible function of a Gateway is constraint on insider access to outside application services (when a trusted computer initiates connection with untrusted computer, Sebes, pg. 163, col. 1, section 3.4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers as per teaching of Sebes to enable CORBA-based application interoperation between trusted and untrusted distributed system (Sebes, Abstract).

13. Regarding claim 20, Meyers shows claim 19 above, but fail to show said trusted computer system can initiate connections with any execution context on said untrusted computer system.

However, Sebes teaches another possible function of a Gateway is constraint on insider access to outside application services (when a trusted computer initiates connection with untrusted computer, Sebes, pg. 163, col. 1, section 3.4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers as per teaching of Sebes to enable CORBA-based application interoperation between trusted and untrusted distributed system (Sebes, Abstract).

14. Claims 3, 21 are rejected under **35 U.S.C. 103(a)** as obvious over Patent No. 5,937,159, Meyers et al.

15. Regarding claims 3, 21 Meyers show claim 1 and 19 above, but fail to show specifically that only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system. However, it would have been obvious to one of ordinary skill in the art at the time of the invention for any untrusted system, regardless of whether a subject has an untrusted application execution context or not, to initiate connection with an external computer system.

16. Claims 10, 12-18, 28, 30-36 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,937,159, Meyers et al. in view of Patent No. 6,473,791, Al-Ghosein et al.

17. Regarding claim 10, Meyers shows a method for controlling access to a trusted computer system comprising:

determining a name of an execution context of an application running on an untrusted system (ftp client, inetd, ftpd, are typically run from untrusted systems, Meyers, col. 14, line 31-34);

determining whether said execution context is trusted or untrusted based on said name (MAC label, Meyers, col. 14, line 36-37);

but fail to show if said execution context is trusted, permitting said application to initiate a connection with said trusted system, and

if said execution context is untrusted, preventing said application from initiating a connection with said trusted computer system.

Al-Ghosein teaches policy objects may return a result using a particular Boolean algebra scheme based on a "Trusted, Completely Trusted and Untrusted" model. In general, "Trusted" corresponds to "Yes" (Al-Ghosein, col. 7, line 55-56). It further teaches an application initiates decision making process when the application needs to determine whether a potentially dangerous action that it is proposed to take is allowed or forbidden in accordance with a policy (initiate connection with trusted system, Al-Ghosein, col. 4, line 64-67, col. 5, line 1).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers as per teaching of Al-Ghosein to use gain the benefit of using a policy to make decision on a proposed action of a system component such as an application.

18. Regarding claim 12, Meyers show claim 10 below, but fail to show specifically that only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system. However, it would have been obvious to one of ordinary skill in the art at the time of the invention for any untrusted system, regardless of whether a subject has an untrusted application execution context or not, to initiate connection with an external computer system.

19. Regarding claim 13 Meyers discloses claim 10 above, and further show a human administrator of said untrusted system assigns said distinctive application execution context names (Meyers, col. 6, line 29-30).

20. Regarding claim 14, Meyers show claim 10 above, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names (name of service, Meyers, col. 12, line 51-52).

21. Regarding claim 15 Meyers shows claim 14 above, and further show said applications cannot change the names of respective execution contexts in which said applications are running (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

22. Regarding claim 16, Meyers shows claim 14 above, and further show said applications cannot change the name of any execution context in said untrusted computer system (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

23. Regarding claim 17, Meyers shows claim 10, above, wherein connections originating on said external system can terminate only at said untrusted system and only at said untrusted execution contexts therein (Session monitor, Meyers, col. 7, line 30-34).

24. Regarding claim 18, Meyers shows claim 10 above, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system (System Boundary, Meyers, col. 4, line 66-67).

25. Regarding claim 28, Meyers shows a system for controlling access to a network comprising:

a trusted computer system (the preferred embodiment is a trusted system, fig. 3);

an untrusted computer system connected to said trusted computer system and to an external computer system (ftp client, inetd, ftpd, are typically run from untrusted systems, Meyers, col. 14, line 31-34), but fail to show wherein said untrusted system includes applications classified as having trusted application execution contexts and untrusted application execution contexts, and

wherein only said trusted application execution contexts can initiate connections with said trusted computer system.

Al-Ghosein teaches policy objects may return a result using a particular Boolean algebra scheme based on a "Trusted, Completely Trusted and Untrusted" model. In general, "Trusted" corresponds to "Yes" (Al-Ghosein, col. 7, line 55-56). It further teaches an application initiates decision making process when the application needs to determine whether a potentially dangerous action that it is proposed to take is allowed or forbidden in accordance with a policy (initiate connection with trusted system, Al-Ghosein, col. 4, line 64-67, col. 5, line 1).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers as per teaching of Al-Ghosein to use gain the benefit of using a policy to make decision on a proposed action of a system component such as an application.

26. Regarding claim 30, Meyers show claim 28 below, but fail to show specifically that only said untrusted application execution contexts on said untrusted system can initiate connections with said external computer system. However, it would have been obvious to one of ordinary skill in the art at the time of the invention for any untrusted system, regardless of whether a subject has an untrusted application execution context or not, to initiate connection with an external computer system.

27. Regarding claim 31, Meyers show claim 28 above, wherein said applications are classified as having said trusted application execution contexts and said untrusted application

execution contexts based on distinctive application execution context names (name of service, Meyers, col. 12, line 51-52).

28. Regarding claim 32 Meyers discloses claim 31 above, and further show a human administrator of said untrusted system assigns said distinctive application execution context names (Meyers, col. 6, line 29-30).

29. Regarding claim 33 Meyers shows claim 31 above, and further show said applications cannot change the names of respective execution contexts in which said applications are running (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

30. Regarding claim 34, Meyers shows claim 28 above, and further show said applications cannot change the name of any execution context in said untrusted computer system (MAC label determines if subject (application) can read an object, write to object, or denied access to the object, Meyers, col. 6, line 9-17).

31. Regarding claim 35, Meyers shows claim 28, above, wherein connections originating on said external system can terminate only at said untrusted system and only at said untrusted execution contexts therein (Session monitor, Meyers, col. 7, line 30-34).

32. Regarding claim 36, Meyers shows claim 28 above, wherein said untrusted application execution contexts are fenced off from said untrusted computer system such that said untrusted application execution application contexts cannot interrogate or change critical system data of said untrusted computer system (System Boundary, Meyers, col. 4, line 66-67).

33. Claims 11, 29 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,937,159, Meyers et al. in view of Patent No. 6,473,791, Al-Ghosein et al. in further view of

"SIGMA: Security for Distributed Object Interoperability Between Trusted and Untrusted Systems", Sebes et al

34. Regarding claim 11, Meyers and Al-Ghosein show claim 10 above, but fail to show said trusted computer system can initiate connections with any execution context on said untrusted computer system.

However, Sebes teaches another possible function of a Gateway is constraint on insider access to outside application services (when a trusted initiating connection with untrusted computer, Sebes, pg. 163, col. 1, section 3.4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers and Al-Ghosein as per teaching of Sebes to enable CORBA-based application interoperation between trusted and untrusted distributed system (Sebes, Abstract).

35. Regarding claim 29, Meyers and Al-Ghosein show claim 28 above, but fail to show said trusted computer system can initiate connections with any execution context on said untrusted computer system.

However, Sebes teaches another possible function of a Gateway is constraint on insider access to outside application services (when a trusted initiating connection with untrusted computer, Sebes, pg. 163, col. 1, section 3.4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Meyers and Al-Ghosein as per teaching of Sebes to enable CORBA-based application interoperation between trusted and untrusted distributed system (Sebes, Abstract).

Conclusion

1. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
5/11/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100